	Georgia Technology Authority	
Title:	**Independent Security Assessments**	
PSG Number:	SS-08-042.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 2
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes requirement for agencies to have IT systems assessed by an independent third-party.	

PURPOSE

Security assessments are an important activity in the risk management process and an agency's information security program. Comprehensive security assessments reveal the extent to which controls are implemented correctly, operating as intended and meeting the required security levels. Assessments are intended to provide management with complete and accurate information regarding the security status of the information systems for which they are responsible; enabling them to make sound risk-based decisions regarding the operations of the information system.

This standard establishes the requirements for conducting valid assessments of state information systems.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

Information systems categorized as HIGH shall be assessed annually by an independent, impartial and qualified third-party.

Assessments shall validate and evaluate the effectiveness of management, operations and technical controls detailed in system security plans and compliance with federal, state and agency regulation, policy and standards.

At an agency's request, GTA OIS shall offer a cost recovery based contract service of pre-qualified security assessment vendors and provide agency support through the Security Assessment and Specialized Services Contract (SASSC) program or agencies may choose to solicit for these services independent of the SASSC program.

Security controls established by NIST SP 800-53/53A supplemented by enterprise security policies and standards shall guide assessment methodologies.

Assessment results and recommendations shall provide Information Owners with the information needed to understand the risks and implications for operating an information system and to assist them in making decisions to mitigate these risks.

The Open Records Act of Georgia has an exception for disclosure of security plans and assessment information (see O.C.G.A. § 50-18-72(15)(A). However, agencies shall provide a copy of the assessment report and resulting planned mitigation steps to the State CISO. In addition, access shall be provided to support legal, state, or federal actions when required; otherwise, access is at the discretion of the agency.

ENTERPRISE RELATED POLICIES, STANDARDS, GUIDELINES

- Security Controls Review and Assessment (Policy)
- Risk Management Framework (Standard)

REFERENCES

- NIST SP 800-12 (chapter 11) Introduction to Computer Security NIST Handbook
- FIPS 200 Minimum Security Requirements for Information Systems
- NIST SP 800-53 Security Controls for Information Systems
- NIST SP 800-53A Guide for Assessing Security Controls
- NIST 800-26 Security Self Assessment Guide for IT Systems
- NIST SP 800-37 Guidelines for Security Certification and Accreditation

Note: The PSG number was changed from S-08-042.01 on September 1, 2008